



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/945,278	08/31/2001	James D. Lyle	SII-600	3819
7590	06/02/2005		EXAMINER	
Alfred A. Equitz GIRARD & EQUITZ LLP 400 Montgomery Street, Suite 1110 San Francisco, CA 94104			LIPMAN, JACOB	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/945,278	LYLE, JAMES D.
	Examiner	Art Unit
	Jacob Lipman	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 31 August 2001.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-62 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) \_\_\_\_\_ is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) 1-60, 61, and 62 are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
     Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
     Paper No(s)/Mail Date. \_\_\_\_\_

5) Notice of Informal Patent Application (PTO-152)

6) Other: \_\_\_\_\_

## DETAILED ACTION

### ***Election/Restrictions***

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
  - I. Claims 1-5 and 28-31, drawn to a communication system that prevents authentication if values do not satisfy criterion, classified in class 713, subclass 169.
  - II. Claims 6-12, drawn to a communication system to generate shared keys, classified in class 713, subclass 171.
  - III. Claims 13-16, drawn to a communication system with an external agent authenticates parties, classified in class 713, subclass 155.
  - IV. Claims 17-20, drawn to a communication system with an external agent generating a shared key, classified in class 380, subclass 279.
  - V. Claims 21-23, drawn to a communication system with an external agent to perform decryption, classified in class 713, subclass 168.
  - VI. Claims 24-27, drawn to a communication system using a value received from another element to create a shared key, classified in class 380, subclass 278.
  - VII. Claims 32-34, drawn to a communication system where a shared secret value determines the shared secret, classified in class 713, subclass 168.
  - VIII. Claims 35-37, drawn to a communication system where a shared secret is a first value and a second value different than the first value, classified in class 713, subclass 168.

- IX. Claim 38, drawn to a communication system with a receiver is a repeater, classified in class 713, subclass 150.
- X. Claims 39-44, drawn to a communication system the receiver receives a pseudo-randomly generated value, employing a Gaussian analog affect, to allow communication, classified in class 380, subclass 268.
- XI. Claim 45, drawn to a communication system preventing substitution of a pseudo-random value, classified in class 380, subclass 268.
- XII. Claims 46-47, drawn to a communication system only acting on encrypted streaming data, classified in class 380, subclass 42.
- XIII. Claims 48-49, drawn to a communication system where a receiver reports updated values to a transmitter to continue receiving encrypted streaming data, classified in class 380, subclass 35.
- XIV. Claims 50-52, drawn to a communication system where a transmitter re-authenticates a receiver, classified in class 713, subclass 201.
- XV. Claims 53-56, drawn to a communication system with tamper protection circuitry, classified in class 713, subclass 194.
- XVI. Claim 57, drawn to a content protection protocol to store shared secrets determined from key vectors, classified in class 380, subclass 264.
- XVII. Claims 58-60, drawn to a content protection protocol to decrypt stored private keys, classified in class 380, subclass 286.
- XVIII. Claim 62-63, drawn to a system for enforcing a revocation list, classified in class 513, subclass 158.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions I-XVIII are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, each invention has separate utility, as briefly outlined above. For example Group I is a system that ensures that authentication values are distinct, with no encryption, while group II needs encryption, but does not assure that authentication values are distinct. Group III uses a separate agent to authenticate 2 parties, and does not need the parties to authenticate each other, as in groups I and II. In group IV, an external system actually generates a shared key, and there is no need for the parties to generate their own shared key. Group V is a system, which needs no shared key and does not ensure that authentication values are distinct. See MPEP § 806.05(d).

3. Because these inventions are distinct for the reasons given above and the search required for each group is different, restriction for examination purposes as indicated is proper.

4. A telephone call was made to Daniel J. Santos on 25 May 2005 at 770-984-2300 to request an oral election to the above restriction requirement, but did not result in an election being made.

5. Applicant is advised that the reply to this requirement to be complete must include an election of the invention to be examined even though the requirement be traversed (37 CFR 1.143).

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob Lipman whose telephone number is 571-272-3837. The examiner can normally be reached on M-Th 7 AM-3 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JL



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100